

Remarks

Reconsideration of the subject application is requested in view of the preceding amendments and the following remarks. Claims 1-21 are in the application. By this Amendment, claims 12, 18, and 21 are cancelled without prejudice. Upon entry of this Amendment, claims 2-11, 13-17, and 19-20 are in the application.

Claims 1, 7, 11, 14-17, and 20 stand rejected as allegedly directed to non-statutory subject matter. Withdrawal of this rejection is requested in view of the amendments to claims 1, 7, 11, 14-17, and 20.

Claims 1, 7, 11, 16, and 20 stand rejected as allegedly indefinite. This rejection is traversed. According to the Office action, the term “almost” in reference to a Montgomery inverse function or procedure in these claims is a relative term that renders these claims indefinite. However, the specification clearly sets forth the precise meaning of an “almost” Montgomery inverse function or procedure. For example, the specification at page 8, lines 1-11, describes the almost Montgomery inverse (“AMI”) as follows:

With reference to Table 1, above, the Kaliski inverse $KINV(a)$ of a can be obtained by first calculating an intermediate value $a^{-1} 2^k \pmod{p}$ in a phase I, and then correcting this intermediate value to obtain the inverse $KINV(a) = a^{-1} 2^n \pmod{p}$ in a phase II. For convenience, the phase I output of the procedure of Table 1 is referred to herein as an “almost” Montgomery inverse (“AMI”) and is defined as:

$$(r, k) = AMI(a) = a^{-1} 2^k \pmod{p},$$

wherein r is referred to as an “intermediate value” of a multiplicative inverse, and 2^k is an intermediate radix. Because the phase I output includes r and k , the value of k is included as a result of the almost Montgomery inverse $AMI()$. The procedure of Phase I is referred to as an “AMI procedure.”

Because an “almost Montgomery inverse” is defined in the specification, one of ordinary skill in the art would be completely apprised of the claim scope, and withdrawal of this rejection is requested.

The rejection of claim 21 is moot in view of the cancellation of claim 21 without prejudice.

In view of the preceding, all claims are believed to be in condition for allowance and action to such end is requested. If any questions remain, the Examiner is invited to telephone the undersigned.

Respectfully submitted,

KLARQUIST SPARKMAN, LLP

By



Michael D. Jones

Registration No. 41,879

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446